

FILED  
IN CLERK'S OFFICE  
U.S. DISTRICT COURT E.D.N.Y.

★ OCT 09 2020 ★

LONG ISLAND OFFICE

CCC

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK

----- X

IN THE MATTER OF AN APPLICATION  
FOR SEARCH WARRANTS FOR:

AFFIDAVIT IN  
SUPPORT OF  
SEARCH WARRANTS

THE PREMISES KNOWN AND DESCRIBED  
AS:

(Fed. R. Crim. P. 41)

A BLACK IPHONE WITH A RED CASE  
("DEVICE 1");

MJ 20-00951  
MJ-20-951

A BLACK AND GRAY KYOCERA CELLULAR  
PHONE MODEL # C6730 ("DEVICE 2");

A BLUE SAMSUNG CELLULAR PHONE  
("DEVICE 3"); AND

A WHITEISH SILVER LG CELLULAR PHONE  
("DEVICE 4"), (COLLECTIVELY, THE  
"SUBJECT TELEPHONES").

----- X

EASTERN DISTRICT OF NEW YORK, SS:

SCOTT SALAMON, being duly sworn, deposes and states that he is a Special Agent with the Department of Homeland Security, Homeland Security Investigations ("HSI"), duly appointed according to law and acting as such. Upon information and belief, there is probable cause to believe that there is located in the PREMISES KNOWN AND DESCRIBED AS: A BLACK IPHONE WITH A RED CASE ("DEVICE 1");

A BLACK AND GRAY KYOCERA CELLULAR PHONE MODEL # C6730 (“DEVICE 2”); A BLUE SAMSUNG CELLULAR PHONE (“DEVICE 3”); A WHITEISH SILVER LG CELLULAR PHONE (“DEVICE 4”), (COLLECTIVELY, THE “SUBJECT TELEPHONES”), further described in Attachments A through D, the things described in Attachments E through H, which constitute evidence, fruits and instrumentalities of a narcotics trafficking and narcotics trafficking conspiracy, in violation of Title 21, United States Code, Sections 846, 841(a)(1) and 841(b)(1)(C) (the “SUBJECT OFFENSES”).

The source of your deponent’s information and the grounds for his belief are as follows:<sup>1</sup>

I. INTRODUCTION

1. I have been a Special Agent with HSI since 2006 and I am currently assigned to the Long Island Violent Gang and Narcotics Task Force. I have participated in investigations into allegations of unlawful possession, distribution and manufacture of controlled substances, including, but not limited to, cocaine and heroin. My narcotics investigations have involved doing surveillance, working with confidential informants and controlled purchases of narcotics. The information contained in this affidavit comes from my discussions with other agents and law enforcement officers, including members of the Nassau County Police Department (“NCPD”) and a review of the evidence related to this investigation. During the course of the investigation, law enforcement used two confidential informants (the “CIs”) to purchase narcotics from DISKIN from inside his home as discussed

---

<sup>1</sup> Because this affidavit is submitted for the limited purpose of establishing probable cause for the search warrants, I have not set forth each and every fact learned during the course of the investigation.

below.<sup>2</sup> Moreover, based on my experience, and in light of the information I have learned during this investigation, I believe there is probable cause that the SUBJECT TELEPHONES were used to communicate with others concerning the SUBJECT OFFENSES, and to receive and store electronic information relating to the names, nicknames, telephone numbers and pager numbers of criminal accomplices.

2. As set forth below, there is probable cause to conclude that BENJI DISKIN has engaged in the SUBJECT OFFENSES and that the SUBJECT TELEPHONES is an instrumentality of those offenses and contains evidence of DISKIN's involvement in the SUBJECT OFFENSES.

## II. PROBABLE CAUSE

3. The United States, including HSI and the NCPD, have been investigating DISKIN for possible violations of the SUBJECT OFFENSES. During the course of the investigation into DISKIN, law enforcement officers utilized the CI to purchase narcotics from DISKIN on two occasions as discussed below.

4. The investigation revealed that DISKIN used cellular telephones to conduct narcotics transactions. Indeed, on two occasions discussed below the CIs, acting at law enforcement's direction, communicated with DISKIN using a cellular telephone for the

---

<sup>2</sup> The CIs have been working with HSI and NCPD for approximately one week. The CIs have pending state narcotics possession cases. In exchange for the information and the cooperation provided by the CIs, the CIs have received monetary compensation and they hope to receive a reduction or dismissal of their state criminal charges. The federal government intends to assist the CIs with trying to get those charges reduced or dismissed because of their cooperation with instant investigation. The CIs have proven to be reliable in that the information provided by them has been corroborated by other sources, including controlled buys of narcotics from DISKIN, surveillance reports and another cooperating source.



purpose of conducting narcotics transactions. I reviewed the communications between the CIs and DISKIN and confirmed that DISKIN utilized cellular telephones to conduct narcotics transactions.

5. On or about October 3, 2020, the CIs placed a call to DISKIN to make arrangements to conduct a narcotics transaction. DISKIN directed the CIs to meet him at his home. The CIs went to the defendant's home and entered the home through the front door. While inside the first floor of the defendant's home, DISKIN sold the CIs a quantity of a brown powdery substance and a white powdery substance, and collected cash from the CIs. The brown powdery substance field-tested positive for the presence of heroin while the white powdery substance field-tested positive for the presence of cocaine. While inside the defendant's home, the CIs observed DISKIN in possession of a larger quantity of those substances. This transaction was recorded using audio and video equipment.

6. On or about October 8, 2020, the CIs placed a call to DISKIN to make arrangements to conduct a narcotics transaction. DISKIN directed the CIs to meet him at his home. The CIs went to the defendant's home and entered through the front door. While inside the first floor of the defendant's home, DISKIN sold the CIs a quantity of a light brown powdery substance, and collected cash from the CIs. The light brown powdery substance field-tested positive for the presence of heroin. While inside the defendant's home, the CIs observed DISKIN in possession of larger quantity of that substance. This transaction was recorded using audio and video equipment

7. On October 8, 2020, the Honorable A. Kathleen Tomlinson, United States Magistrate Judge, signed a warrant authorizing the search the defendant's home. The next day, on October 9, 2020, law enforcement officers and I executed that search warrant.

8. When law enforcement entered the defendant's home, they found the defendant in the bathroom with his hand in the toilet bowl attempting to flush drugs down the toilet. He was directed to remove his hand from the toilet, and law enforcement found a bag containing a hard-rock like substance, which field-tested positive for the presence of cocaine base. Law enforcement removed the toilet bowl from the floor and recovered a bag containing a brown-powdery substance, which field-tested positive for the presence of heroin. Law enforcement subsequently weighed the cocaine base and heroin and determined that those substances weighed approximately 25 grams and 125 grams, respectively. In addition, during the court-authorized search of the defendant's home, law enforcement officers recovered the SUBJECT TELEPHONES, approximately five pounds of marijuana, a scale commonly used to weigh drugs, drug packaging materials, \$18,451 in United States currency, among other things. Based on my training and experience and discussions with other law enforcement officers, the quantity of heroin and cocaine base recovered from the defendant's home was consistent with distribution.

9. The defendant BENJI DISKIN was placed under arrest and read his Miranda rights. The defendant waived those Miranda rights and agreed to be interviewed. During that interview, the defendant admitted, in sum and substance, that: he purchased the heroin and cocaine base the day before the search warrant. He stated that he purchased the cocaine base for approximately \$1,200 to 1,300. While he denied selling drugs to

individuals, he did admit that he distributed narcotics to individuals. Specifically, the defendant admitted that he distributed narcotics to women, who, in exchange for the narcotics, would provide him with sexual favors.

10. Based on my training and experience, I am familiar with the typical distribution and trafficking methods used by drug dealers and traffickers, including the manufacture and distribution of narcotics.

11. In a substantial number of drug investigations, the following kinds of drug-related evidence have typically been recovered:

a. Members of drug organizations often maintain close at hand the addresses and telephone numbers of their criminal associates, including information pertaining to their sources of supply and customers, in mobile telephones.

b. Records of calls to telephones (landlines and mobile telephones). Such records constitute important corroborative evidence in drug conspiracy cases because the defendants call one another regularly, especially just before and after an incident involving an act committed in furtherance of the conspiracy.

c. Drug traffickers frequently maintain records, receipts, notes, ledgers, and other electronic documents relating to the ordering, sale and distribution of drugs. Such records are generally maintained where the traffickers have ready access to them, such as the trafficker's cellular telephones. Such records are maintained in digital format on cellular phones, which are capable of holding digital data.

d. Drug traffickers frequently maintain financial records evidencing the deposit and transfer of monies in their homes. Such records are generally



maintained where the traffickers have ready access to them, such as the trafficker's cellular telephones. Such records are maintained in digital format on cellular phones, which are capable of holding digital data.

e. Based upon my training and experience, as well as my discussions with other law enforcement officers, I am aware that it is generally a common practice for drug traffickers to maintain records relating to their drug trafficking activities. Because drug traffickers will "front" (that is, sell on consignment) controlled substances to their clients, or alternatively, will be "fronted" controlled substances from their suppliers, such record-keeping is necessary to keep track of amounts paid and owed, and such records will also be maintained close at hand so as to readily ascertain current balances. Often drug traffickers keep "pay and owe" records to show balances due for drugs sold in the past ("pay") and for payments expected ("owe") as to the trafficker's supplier and the trafficker's dealer(s). Additionally, drug traffickers must maintain telephone and address listings of clients and suppliers and keep them immediately available in order to efficiently conduct their trafficking business. Such records are maintained in digital format on cellular telephones, which are capable of holding digital data.

12. Also, I know, from both my professional and personal experiences, that people often maintain multiple cellular telephones and other cellular telephones capable of holding digital data used to facilitate drug activities.

13. Based on my training, experience and discussions with other law enforcement officers, I understand that individuals involved in the distribution and possession with intent to distribute narcotics, often do not act alone and often communicate

with co-conspirators by means of cellular telephones such as the SUBJECT TELEPHONES.

Such persons commonly maintain records that reflect names, addresses, or telephone numbers of their associates in their cellular telephones. They also commonly maintain records of communications such as call logs, chats and text messages in their cellular telephones. They commonly take photographs of themselves, their associates, or their property using their cellular telephones. These individuals usually maintain these records of communication and photographs in their possession and in their cellular telephones.

#### TECHNICAL TERMS

14. As used herein, the following terms have the following meanings:

15. Wireless telephone (or mobile or cellular telephone): A handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving and storing text messages and email; taking, sending, receiving and storing still photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device, and a wide variety of applications, also known as “apps,” which



may store the user's preferences and other data. Such apps may include Facebook, Twitter, and other social media services.

16. Based on my research, I understand that the SUBJECT TELEPHONES provide not only phone and text message services, but can also be used to send and receive emails; access the Internet; track GPS data; take, store and share photographs and videos; and use a wide variety of apps. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the SUBJECT TELEPHONES.

#### TECHNICAL BACKGROUND

17. As further described in Attachments E through H, this application seeks permission to locate not only data that might serve as direct evidence of the crimes described on the warrants, but also for forensic electronic evidence that establishes how the SUBJECT TELEPHONES were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence can be recovered from the SUBJECT TELEPHONES because:

a. Data on an electronic device can provide evidence of a file that was once on the device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the device that show what tasks and processes were recently active. Web browsers, email programs, and instant messaging/"chat" programs store configuration information on the device that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such

as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the device was in use. Electronic devices can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on an electronic device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, instant messaging or chat logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the electronic device at a relevant time.

c. A person with appropriate familiarity with how an electronic device works can, after examining this forensic evidence in its proper context, draw conclusions about how devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on an electronic device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, such evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on an electronic device is evidence may depend on other information stored on the device and the application of

knowledge about how the device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding user attribution evidence, sometimes it is necessary to establish that a particular thing is not present on an electronic device. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

18. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, the warrants I am applying for would permit the examination of the SUBJECT TELEPHONES consistent with the warrants. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

19. Because this application seeks only permission to examine the SUBJECT TELEPHONES, which are already in law enforcement's possession, the execution of the warrants does not involve intrusion into a physical location. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrants at any time in the day or night.

#### CONCLUSION


20. Based on the foregoing, there is probable cause to believe that there is located in the SUBJECT TELEPHONES, further described in Attachments A through D, the things described in Attachments E through H, which constitute evidence, fruits and



instrumentalities of the SUBJECT OFFENSES. Accordingly, the Court should issue the requested warrants.

21. WHEREFORE, your deponent respectfully requests that search warrants be issued for the PREMISES KNOWN AND DESCRIBED AS: A BLACK IPHONE WITH A RED CASE ("DEVICE 1"); A BLACK AND GRAY KYOCERA CELLULAR PHONE MODEL # C6730 ("DEVICE 2"); A BLUE SAMSUNG CELLULAR PHONE ("DEVICE 3"); A WHITEISH SILVER LG CELLULAR PHONE ("DEVICE 4"), (COLLECTIVELY, THE "SUBJECT TELEPHONES"),

Dated: Central Islip, New York  
October 9, 2020

  
\_\_\_\_\_  
SCOTT SALAMON  
Special Agent  
HSI  
(Application by Telephone and/or  
FaceTime)

Sworn to before me this  
9th day of October, 2020

/s/ AK Tomlinson  
THE HONORABLE A. KATHLEEN TOMLINSON  
UNITED STATES MAGISTRATE JUDGE  
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

Property To Be Searched

The property to be searched is a BLACK IPHONE WITH A RED CASE (“DEVICE 1”), seized on or about October 9, 2020, from BENJI DISKIN’s home in Nassau County, New York. The warrant authorizes the forensic examination of DEVICE #1 for the purpose of identifying the electronically stored information described in Attachment E.

ATTACHMENT B

Property To Be Searched

The property to be searched is a BLACK AND GRAY KYOCERA CELLULAR PHONE MODEL # C6730 (“DEVICE 2”), seized on or about October 9, 2020, from BENJI DISKIN’s home in Nassau County, New York. The warrant authorizes the forensic examination of DEVICE #2 for the purpose of identifying the electronically stored information described in Attachment F.



ATTACHMENT C

Property To Be Searched

The property to be searched is a BLUE SAMSUNG CELLULAR PHONE (“DEVICE #3”), seized on or about October 9, 2020, from BENJI DISKIN’s home in Nassau County, New York. The warrant authorizes the forensic examination of DEVICE #3 for the purpose of identifying the electronically stored information described in Attachment G.

ATTACHMENT D  
Property To Be Searched

The property to be searched is a WHITEISH SILVER LG CELLULAR PHONE (“DEVICE #4”), seized on or about October 9, 2020, from BENJI DISKIN’s home in Nassau County, New York. The warrant authorizes the forensic examination of DEVICE #4 for the purpose of identifying the electronically stored information described in Attachment H.

ATTACHMENT E

Particular Things To Be Seized

All information obtained from DEVICE #1 will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the purpose of identifying and seizing all information described below that constitutes evidence, fruits, or instrumentalities of a conspiracy to distribute and possess with intent to distribute controlled substances, in violation of Title 21, United States Code, Sections 841(b)(1)(A) and 846, including:

1. All records and information on DEVICE #1 described in Attachment A, including (a) names and telephone numbers, as well as the contents of all call logs, contact lists, and (b) text messages, emails (including those sent, received, deleted and drafted), instant messages, photographs, videos, social media account activity (including postings and messages), Internet activity (including browser history, web page logs, and search terms entered by the user), and other electronic media constituting evidence, fruits, or instrumentalities of the violations described above.

2. Evidence of user attribution showing who used or owned DEVICE #1 at the time the things described in this warrant were created, edited, or deleted, such as, for example, logs, phonebooks, saved usernames and passwords, documents, and browsing history;



3. Evidence of software that would allow others to control DEVICE #1, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
4. Evidence of the lack of such malicious software;
5. Evidence of the attachment to DEVICE #1 of other storage devices or similar containers for electronic evidence;
6. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from DEVICE #1;
7. Evidence of the times DEVICE #1 were used;
8. Passwords, encryption keys, and other access devices that may be necessary to access DEVICE #1; and
9. Contextual information necessary to understand the evidence described in this attachment, all of which constitute evidence, fruits and instrumentalities of the violations described above.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

ATTACHMENT F

Particular Things To Be Seized

All information obtained from DEVICE #2 will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the purpose of identifying and seizing all information described below that constitutes evidence, fruits, or instrumentalities of a conspiracy to distribute and possess with intent to distribute controlled substances, in violation of Title 21, United States Code, Sections 841(b)(1)(A) and 846, including:

1. All records and information on DEVICE #2 described in Attachment B, including (a) names and telephone numbers, as well as the contents of all call logs, contact lists, and (b) text messages, emails (including those sent, received, deleted and drafted), instant messages, photographs, videos, social media account activity (including postings and messages), Internet activity (including browser history, web page logs, and search terms entered by the user), and other electronic media constituting evidence, fruits, or instrumentalities of the violations described above.

2. Evidence of user attribution showing who used or owned DEVICE #2 at the time the things described in this warrant were created, edited, or deleted, such as, for example, logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Evidence of software that would allow others to control DEVICE #2 such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
4. Evidence of the lack of such malicious software;
5. Evidence of the attachment to DEVICE #2 of other storage devices or similar containers for electronic evidence;
6. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from DEVICE #2;
7. Evidence of the times DEVICE #2 were used;
8. Passwords, encryption keys, and other access devices that may be necessary to access DEVICE #2; and
9. Contextual information necessary to understand the evidence described in this attachment, all of which constitute evidence, fruits and instrumentalities of the violations described above.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

ATTACHMENT G

Particular Things To Be Seized

All information obtained from DEVICE #3 will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the purpose of identifying and seizing all information described below that constitutes evidence, fruits, or instrumentalities of a conspiracy to distribute and possess with intent to distribute controlled substances, in violation of Title 21, United States Code, Sections 841(b)(1)(A) and 846, respectively, including:

1. All records and information on DEVICE #3 described in Attachment C, including (a) names and telephone numbers, as well as the contents of all call logs, contact lists, and (b) text messages, emails (including those sent, received, deleted and drafted), instant messages, photographs, videos, social media account activity (including postings and messages), Internet activity (including browser history, web page logs, and search terms entered by the user), and other electronic media constituting evidence, fruits, or instrumentalities of the violations described above.

2. Evidence of user attribution showing who used or owned DEVICE #3 at the time the things described in this warrant were created, edited, or deleted, such as, for example, logs, phonebooks, saved usernames and passwords, documents, and browsing history;



3. Evidence of software that would allow others to control DEVICE #3, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
4. Evidence of the lack of such malicious software;
5. Evidence of the attachment to DEVICE #3 of other storage devices or similar containers for electronic evidence;
6. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from DEVICE #3;
7. Evidence of the times DEVICE #3 were used;
8. Passwords, encryption keys, and other access devices that may be necessary to access DEVICE #3; and
9. Contextual information necessary to understand the evidence described in this attachment, all of which constitute evidence, fruits and instrumentalities of the violations described above.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

ATTACHMENT H

Particular Things To Be Seized

All information obtained from DEVICE #4 will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the purpose of identifying and seizing all information described below that constitutes evidence, fruits, or instrumentalities of a conspiracy to distribute and possess with intent to distribute controlled substances, in violation of Title 21, United States Code, Sections 841(b)(1)(A) and 846, respectively, including:

10. All records and information on DEVICE #4 described in Attachment C, including (a) names and telephone numbers, as well as the contents of all call logs, contact lists, and (b) text messages, emails (including those sent, received, deleted and drafted), instant messages, photographs, videos, social media account activity (including postings and messages), Internet activity (including browser history, web page logs, and search terms entered by the user), and other electronic media constituting evidence, fruits, or instrumentalities of the violations described above.

11. Evidence of user attribution showing who used or owned DEVICE #4 at the time the things described in this warrant were created, edited, or deleted, such as, for example, logs, phonebooks, saved usernames and passwords, documents, and browsing history;

12. Evidence of software that would allow others to control DEVICE #4, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
13. Evidence of the lack of such malicious software;
14. Evidence of the attachment to DEVICE #4 of other storage devices or similar containers for electronic evidence;
15. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from DEVICE #4;
16. Evidence of the times DEVICE #4 were used;
17. Passwords, encryption keys, and other access devices that may be necessary to access DEVICE #4; and
18. Contextual information necessary to understand the evidence described in this attachment, all of which constitute evidence, fruits and instrumentalities of the violations described above.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.